



(11)

EP 2 264 940 B1

(12)

EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention
of the grant of the patent:
27.01.2016 Bulletin 2016/04

(51) Int Cl.:
H04L 9/32 ^(2006.01) **H04L 12/24** ^(2006.01)
H04L 29/06 ^(2006.01)

(21) Application number: **09716567.4**

(86) International application number:
PCT/KR2009/000990

(22) Date of filing: **02.03.2009**

(87) International publication number:
WO 2009/110703 (11.09.2009 Gazette 2009/37)

(54) **AUTHENTICATION INFORMATION MANAGEMENT METHOD IN HOME NETWORK AND AN APPARATUS THEREFOR**

VERFAHREN ZUR VERWALTUNG VON AUTHENTIFIZIERUNGSMITTELSINFORMATIONEN IN EINEM HEIMNETZ UND GERÄT DAFÜR

PROCÉDÉ DE GESTION D'INFORMATIONS D'AUTHENTIFICATION DANS UN RÉSEAU DOMESTIQUE ET APPAREIL UTILISÉ

(84) Designated Contracting States:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL
PT RO SE SI SK TR**

(30) Priority: **04.03.2008 US 33485 P**
21.07.2008 KR 20080070788

(43) Date of publication of application:
22.12.2010 Bulletin 2010/51

(73) Proprietor: **Samsung Electronics Co., Ltd.**
Suwon-si, Gyeonggi-do, 443-742 (KR)

(72) Inventors:
• **CHO, Seong-Ho**
Yongin-si
Gyeonggi-do 446-712 (KR)
• **KIM, Hyung-Shick**
Yongin-si
Gyeonggi-do 446-712 (KR)

(74) Representative: **Birchenough, Lewis et al**
HGF Limited
Saviour House
9 St Saviourgate
York YO1 8NQ (GB)

(56) References cited:
WO-A2-2007/057758 JP-A- 2007 074 390
KR-A- 20070 062 199 US-A1- 2004 128 509
US-A1- 2006 174 105

- **YUN-KYUNG LEE ET AL: "Home Network Device Authentication: Device Authentication Framework and Device Certificate Profile", 16 June 2007 (2007-06-16), ADVANCES IN WEB AND NETWORK TECHNOLOGIES, AND INFORMATION MANAGEMENT; [LECTURE NOTES IN COMPUTER SCIENCE], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 573 - 582, XP019095187, ISBN: 978-3-540-72908-2 * the whole document ***
- **DAN FORSBERG ED - GUENTHER LIEBL ET AL: "Use Cases of Implicit Authentication and Key Establishment with Sender and Receiver ID Binding", WORLD OF WIRELESS, MOBILE AND MULTIMEDIA NETWORKS, 2007. WOWMOM 2007. IEEE INTERNATIONAL SYMPOSIUM ON A, IEEE, PI, 1 June 2007 (2007-06-01), pages 1-8, XP031149204, ISBN: 978-1-4244-0992-1**
- **Charles Knouse: "SAML Implementation Guidelines", , 27 August 2004 (2004-08-27), pages 1-40, XP55036980, Retrieved from the Internet: URL: <http://xml.coverpages.org/SAML-ImplementationGuidelinesV01-8958.pdf> [retrieved on 2012-09-03]**
- **NAKAKITA H ET AL: "A STUDY ON SECURE WIRELESS NETWORKS CONSISTING OF HOME APPLIANCES", IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, IEEE SERVICE CENTER, NEW YORK, NY, US, vol. 49, no. 2, 1 May 2003 (2003-05-01), pages 375-381, XP001171298, ISSN: 0098-3063, DOI: 10.1109/TCE.2003.1209528**

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 2 264 940 B1

Description

Technical Field

[0001] Methods and apparatuses consistent with the present invention relate to providing secure communication between devices in a home network, and more particularly, to managing authentication information in a home network, which functions to provide secure communication between a control device and a controlled device.

Background Art

[0002] Due to the development of home networks, an existing personal computer (PC)-centered network environment in the home has expanded into a network environment which includes electronic devices using various lower network technologies. In this regard, there was a necessity to develop a technology that can network the electronic devices with a unified system by using Internet Protocol (IP) protocol, thus, a home network middleware technology such as Universal Plug and Play (UPnP) technology has been presented.

[0003] The UPnP technology is based on a distributed and open networking architecture, and allows peer-to-peer networking of each electronic device in a home network, without central administration.

[0004] In general, in home network middleware, a controlled device such as a UPnP device can model its service into actions and state variables, and a control device such as a UPnP Control Point (CP) can automatically discover the controlled device and then use the service.

[0005] In order to configure a home network, a security system must be built to prevent a device from being manipulated by an external intruder. The UPnP technology provides an UPnP security console standard and an UPnP device security standard so as to present a security function between a CP and the device. The standards provide security functions such as discrimination of an UPnP control message, integrity, and authentication.

[0006] Wi-Fi Protected Setup (WPS) is a standard for easy and secure establishment of a wireless home network, and is presented by the Wi-Fi Alliance. The goal of the WPS is to simplify the process of connecting a home device to a wireless network, and to protect a home network from an external attack. A mandatory model among WPS models is a Product Identification Number (PIN) method which arranges the input of a serial number of a new device to Registrar of a network so as to start a security session, wherein the serial number is allocated to the new device at the time of manufacture. The security session is composed of eight Extensible Authentication Protocol (EAP) messages.

[0007] Also, Transport Layer Security (TLS) is the Internet Engineering Task Force (IETF) standard aiming to provide end-to-end security on a transport layer. End-to-end authentication is provided by a public key algo-

rithm and an X.509 public key certificate. End-to-end confidentiality is provided by a secret key (a session key) shared by using the Handshake Protocol. Also, end-to-end integrity is provided by a message authentication code (MAC).

[0008] A technique for home network device authentication is described in Yun-Kyung Lee et al, "Home Network Device Authentication: Device Authentication Framework and Device Certificate Profile", Advances in Web and Network Technologies, and Information Management, Lecture Notes in Computer Science, Springer Berlin Heidelberg, Pages 573-582, ISBN 978-3-540-72908-2.

[0009] A technique for establishing a key for secure communication between two parties derived from an initial key and identity information is described in Dan Forsberg, "Use Cases of Implicit Authentication and Key Establishment with Sender and Receiver ID Binding", World of Wireless, Mobile and Multimedia Networks, 1 June 2007, IEEE International Symposium on, pages 1-8, ISBN 978-1-4244-0992-1

Technical Solution

[0010] The present invention provides a method of managing authentication information in a home network and a security manager apparatus for the method which provides a secure communication between each of devices in the home network.

Advantageous Effects

[0011] According to the current exemplary embodiment, if PINs corresponding to the number of control devices are input to the security manager 110, the control devices may be efficiently registered in the security manager 110.

[0012] According to the current exemplary embodiment, it is possible to efficiently revoke a certificate of a device. That is, when the CRL is distributed, it is not necessary to set a secure channel for each of the registered devices and to transmit the CRL to each of the registered devices via unicast transmission but it is possible to transmit the CRL to each of the registered devices via single broadcast/multicast transmission. At this time, by using the SSK in calculation of the MAC value, the integrity of the CRL may be ensured.

[0013] According to the current exemplary embodiment, in order to provide a secure communication between each of devices in a home network, a separate apparatus such as a security console based on an UPnP security architecture and a separate protocol such as a WPS protocol are not required, and also an additional out-of-band protocol is not required to be implemented, except for the TLS. That is, it is possible to easily implement communication security by slightly changing the existing TLS that is widely used. Also, the TLS is implemented by using a pre-shared symmetric key instead of

using a public key certificate, thus, a complicated calculation necessary for an authentication process using a public key may be avoided.

Description of drawings

[0014] The above and other aspects of the present invention will become more apparent by describing in detail exemplary embodiments thereof with reference to the attached drawings in which:

FIG. 1 is a diagram illustrating a method of registering a control device to a security manager according to an exemplary embodiment of the present invention; FIG. 2 is a diagram illustrating a method of registering a controlled device to a security manager via a control device according to an exemplary embodiment of the present invention;

FIG. 3 is a diagram illustrating a method of establishing a Secure Authenticated Channel (SAC) between a control device and a controlled device according to an exemplary embodiment of the present invention;

FIG. 4 is a diagram illustrating a method of registering a new user to a security manager via a control device according to an exemplary embodiment of the present invention;

FIG. 5 is a diagram illustrating a method of authenticating a user by using a security manager, wherein the method is performed by a controlled device, according to an exemplary embodiment of the present invention;

FIG. 6 is a diagram illustrating a method of implementing Transport Layer Security Pre-Shared Key ciphersuites (TLS-PSK) by using a pre-shared Product Identification Number (PIN) value according to an exemplary embodiment of the present invention; FIG. 7 is a diagram illustrating a method of synchronizing authentication information between a security manager and a sub-security manager according to an exemplary embodiment of the present invention; and

FIG. 8 is a block diagram of a structure of a security manager apparatus, according to an exemplary embodiment of the present invention.

Best Mode

[0015] According to an aspect of the present invention, there is provided a method for managing authentication information in a home network comprising a control device and a controlled device, the method comprising the steps of: receiving, by a Security Manager, PIN information that is externally input and is an identifier allocated to the control device or the controlled device at a time of manufacture; and transmitting authentication information from the Security Manager to the control device or the controlled device via a SAC generated by using a Trans-

port Layer Security Pre-Shared Key ciphersuites (TLS-PSK) protocol implemented by using the PIN information, wherein the authentication information is necessary for a user to control the controlled device via the control device.

[0016] The method may further include establishing the SAC by using a TLS-PSK protocol implemented by using a TLS session resumption protocol which uses a randomly generated value as a session identification (ID).

[0017] The establishing the SAC may include the operations of calculating a hash value by using a pre-master secretly generated from the PIN information; and transmitting the hash value to the control device or the controlled device, whereby the control device or the controlled device authenticates the Security Manager.

[0018] The authentication information may include a certificate about the control device or the controlled device, a security key shared in the home network, and user authentication information about a user.

[0019] The method may further include the operations of generating the certificate about the control device or the controlled device; and receiving the user authentication information from the control device via the SAC.

[0020] The method may further include the operations of adding the certificate to a Certificate Revocation List (CRL), wherein the certificate is about a device corresponding to an identifier that is externally input or a device that is not discovered during a predetermined period of time; and distributing the CRL to a plurality of registered control devices and controlled devices.

[0021] The method may further include the operations of changing or deleting user authentication information that is externally input; and distributing the changed or deleted user authentication information to the plurality of registered control devices and controlled devices.

[0022] The operation of distributing the CRL may include the operations of generating an MAC value by using the security key shared in the home network, and transmitting the MAC value along with a message via broadcast or multicast transmission.

[0023] The method may be performed by the Security Manager, and the Security Manager may be selected from among a plurality of security managers according to a predetermined priority order.

[0024] The method may further include: requesting update of information to a sub-security manager, which manages authentication information in a lower layer of management, via the control device if authentication information is newly added, changed or deleted; and establishing the SAC with the sub-security manager; and transmitting the newly added, changed or deleted authentication information to the sub-security manager.

[0025] According to another aspect of the present invention, there is provided a computer readable recording medium having recorded thereon a program for executing the method.

[0026] According to another aspect of the present in-

vention, there is provided an apparatus for managing authentication information in a home network comprising a control device and a controlled device, the apparatus comprising: a user interface unit for receiving PIN information that is externally input and is an identifier allocated to the control device or the controlled device at a time of manufacture; and an authentication information transmitting unit for transmitting authentication information to the control device or the controlled device via a SAC generated by using a TLS-PSK protocol implemented by using the PIN information, wherein the authentication information is necessary for a user to control the controlled device via the control device.

Mode for invention

[0027] The present invention will now be described more fully with reference to the accompanying drawings, in which exemplary embodiments of the invention are shown. Like reference numerals in the drawings denote like elements, and in the drawings, the sizes of the elements may be exaggerated for clarity.

[0028] FIG. 1 is a diagram illustrating a method of registering a control device 100 to a security manager 110 according to an exemplary embodiment of the present invention.

[0029] In the current exemplary embodiment, the control device 100 may be a CP and a controlled device may be a UPnP device in a UPnP home network. In order to implement the present invention, new actions and new state variables may be defined in the UPnP device.

[0030] The security manager 110 manages authentication information for each of devices and users in a home network, and functions to transmit authentication information to the control device 100 or the controlled device via a Secure Authenticated Channel (SAC).

[0031] The control device 100, which is not yet registered, discovers the security manager 110 (operation 121). In the case where a plurality of security managers exist, the control device 100 selects a security manager according to a priority order. For the priority order, information about tree hierarchy between each of the security managers, a priority order included in a discovered security manager, or the like may be used.

[0032] PIN Information of the control device 100 is externally input to the security manager 110 (operation 122). The control device 100 and the security manager 110 establishes an SAC by using a TLS-PSK protocol implemented by using the PIN shared between the control device 100 and the security manager 110 (operation 123). At this time, the PIN may extend to have a length sufficient to meet a requirement of TLS-PSK by using a random number generator.

[0033] Here, the PIN indicates an identifier allocated to the control device 100 at the time of manufacture. Such a PIN may be internally or externally recorded in the control device 100, or may be separately provided to a user purchasing the control device 100.

[0034] TLS (Transport Layer Security) is a protocol used in Internet communication security. The TLS-PSK protocol is designed to implement TLS by using a pre-shared symmetric key, instead of using a public key certificate, and to avoid a complicated calculation necessary for an authentication process using a public key. The SAC may be established between the control device and the controlled device by using the TLS-PSK protocol. The TLS and the TLS-PSK protocols are respectively defined in Request for Comments (RFC) 4346 and RFC 4279, and thus, detailed descriptions thereof will be omitted here.

[0035] The security manager 110 generates a certificate of the control device 100 (operation 124). The certificate of the control device 100 includes the identifier of the control device 100. The identifier of the control device 100 may be a value obtained by applying a one-way hash function to the PIN of the control device 100. The control device 100 receives authentication information from the security manager 110 via an TriggerSetSecret interface call of the security manager 110 (operation 125), wherein the authentication information includes a Shared Secret Key (SSK) that is a security key shared in a home network, the certificate of the control device 100, and the like. At this time, the authentication information is securely transmitted by using a TLS-PSK based out-of-band protocol (operation 126). For example, the TLS-PSK based out-of-band protocol may be a Hypertext Transfer Protocol (HTTP) protocol. The security manager 110 stores the identifier and the authentication information of the control device 100 that is newly added.

[0036] According to the current exemplary embodiment, if PINs corresponding to the number of control devices are input to the security manager 110, the control devices may be efficiently registered in the security manager 110.

[0037] FIG. 2 is a diagram illustrating a method of registering a controlled device 210 to a security manager 220 via a control device 200 according to an exemplary embodiment of the present invention.

[0038] The control device 200 discovers the security manager 220 and the controlled device 210 that is not yet registered (operation 231).

[0039] PIN Information of the control device 200 is externally input to the security manager 220 (operation 232). The controlled device 210 and the security manager 220 establishes an SAC by using a TLS-PSK protocol implemented by using a PIN shared between the controlled device 210 and the security manager 220 (operation 233). The security manager 220 generates a certificate of the controlled device 210 (operation 234). The certificate of the controlled device 210 includes an identifier of the controlled device 210. The identifier of the controlled device 210 may be a value obtained by applying a one-way hash function to a PIN of the controlled device 210. The control device 200 may call a TriggerSetSecret() interface of the security manager 220 (operation 235), thereby enabling the security manager 220

to deliver the generated certificate of the controlled device 210 to the corresponding controlled device 210. At this time, authentication information including an SSK, the certificate, and the like is securely transmitted by using a TLS-PSK based out-of-band protocol (operation 236). For example, the TLS-PSK based out-of-band protocol may be an HTTP protocol. The security manager 220 stores the identifier and the authentication information of the controlled device 210 that is newly added.

[0040] According to the current exemplary embodiment, if PINs corresponding to the number of controlled devices are input to the security manager 220, the controlled devices may be efficiently registered in the security manager 220.

[0041] In the case where the control device 200 or the controlled device 210 is removed from a home network, the certificate of the control device 200 or the controlled device 210 to be removed should be invalidated. In this regard, since the SSK is used only for determining integrity of a message, it is not particularly necessary to update the SSK.

[0042] The security manager 220 may receive an identifier of a device to be removed from a user via a user interface (UI) of the control device 200 or an UI of the controlled device 210, and may remove the device from a device list. Otherwise, a device, which has not been discovered during a predetermined period of time, may be removed from the device list that is managed by the security manager 220.

[0043] The security manager 220 adds certificate information about a certificate of the removed device to a CRL. The security manager 220 distributes the CRL to registered devices. Here, the security manager 220 generates a MAC value by using the SSK, and transmits the MAC value along with the CRL via broadcast/multicast transmission. By doing so, integrity of the CRL may be ensured.

[0044] According to the current exemplary embodiment, it is possible to efficiently revoke a certificate of a device. That is, when the CRL is distributed, it is not necessary to set a secure channel for each of the registered devices and to transmit the CRL to each of the registered devices via unicast transmission but it is possible to transmit the CRL to each of the registered devices via single broadcast/multicast transmission. At this time, by using the SSK in calculation of the MAC value, the integrity of the CRL may be ensured.

[0045] FIG. 3 is a diagram illustrating a method of generating an SAC between a control device 310 and a controlled device 320 according to an exemplary embodiment of the present invention.

[0046] In the current exemplary embodiment, it is assumed that the control device 310 and the controlled device 320 are already registered in a security manager (operation 331).

[0047] The control device 310 discovers the controlled device 320 (operation 332). The control device 310 calls a RequestSAC() interface (operation 333), thereby start-

ing TLS according to a certificate (operation 334). In order to verify validity of the certificate, a validity period of the certificate may be checked, whether the certificate is registered in a CRL may be checked, or the validity of the certificate may be provided from an Online Certificate Status Protocol (OCSP) service of a security manager.

[0048] FIG. 4 is a diagram illustrating a method of registering a new user to a security manager 420 via a control device 410 according to an exemplary embodiment of the present invention.

[0049] The control device 410 discovers the security manager 420 (operation 431). PIN information of the control device 410 is externally input to the security manager 420 (operation 432). The control device 410 and the security manager 420 establish an SAC by using a TLS-PSK protocol implemented by using a PIN shared between the control device 410 and the security manager 420 (operation 433).

[0050] The control device 410 registers a user account to the security manager 420 via a RegisterUser interface of the security manager 420 (operation 435). At this time, user account information may be stored in the control device 410 for a use at a later time. Information requiring security, such as a password of the user account is securely transmitted via the SAC (operation 435). In the case where the SAC is not established, the RegisterUser interface may not be called. The security manager 420 stores the user account information and password information (operation 436).

[0051] Meanwhile, in the case where a specific user account and password information are changed or deleted, the specific user account and the password information have to be changed in or deleted from a security manager and devices which store the specific user account and the password information.

[0052] A user inputs an identifier of a user account to be changed or deleted via a separate UI of the control device 410 or a separate UI of the security manager 420. The security manager 420 changes or deletes information about the input user account, and distributes the changed or deleted information to devices registered in a home network. At this time, the security manager 420 generates an MAC value by using an SSK, and transmits the MAC value along with the changed or deleted information via broadcast/multicast transmission. By doing so, integrity of the changed or deleted information may be ensured.

[0053] FIG. 5 is a diagram illustrating a method of authenticating a user by using a security manager 520, wherein the method is performed by a controlled device 530, according to an exemplary embodiment of the present invention.

[0054] The user calls an arbitrary interface of the controlled device 530 by using a control device 510. In the case where the arbitrary interface requires user authentication, the control device 510 requests account information to the user via a UI (operation 542). The control device 510 receives ID/password information from the

user via the corresponding UI.

[0055] The control device 510 calls an `UserAuthentication()` interface, thereby securely transferring the received ID/password information to the controlled device 530 via a TLS session (operation 543). With respect to the user authentication, if the controlled device 530 has user authentication information stored therein, the controlled device 530 directly performs an authentication process. If the controlled device 530 is not enabled to directly perform the authentication process, the controlled device 530 notices an error via eventing. That is, in the case where the user authentication is not performed due to the controlled device 530 not having user authentication information stored therein (operation 544), the controlled device 530 notices non-performance of the user authentication via eventing of `AuthenticationStatus()` (operation 545), and then the control device 510 calls a `TransferUserAuthentication()` interface (operation 546) so as to request the security manager 520 to transfer the user authentication information to the corresponding controlled device 530. The controlled device 530 receives the user authentication information from the security manager 520 (operation 547), and then performs the user authentication. If required, the controlled device 530 may store the user authentication information (operation 548) and may use it again at a later time when the user authentication is required. An authentication result may be transmitted to the control device 510 via the `AuthenticationStatus()` of the controlled device 530 (operation 549).

[0056] FIG. 6 is a diagram illustrating a method of implementing TLS-PSK by using a pre-shared PIN value according to an exemplary embodiment of the present invention.

[0057] The TLS-PSK may be implemented according to RFC 4279. However, most devices implementing TLS 1.1 do not support the RFC 4279. Thus, it is necessary to implement the TLS-PSK in the devices not supporting the RFC 4279 so as to minimize a change in a protocol stack of the existing devices using the TLS protocol. In the current exemplary embodiment, the method of implementing the TLS-PSK by using a TLS session resumption protocol will now be described. Such TLS-PSK may be used replacing a method of generating a channel key according to a Diffie-Hellman key exchange likewise in Wi-Fi Protected Setup (WPS). When a server and a client complete an authentication via TLS, a session is ended. After that, when the session resumes, a session resumption protocol is used to omit an authentication process by using a session ID so as not to repeat the performing of public key calculations (e.g., a Rivest-Shamir-Adleman (RSA) algorithm).

[0058] A pre-shared PIN is extended by using a random number generator or a hash function so that a Pre-master secret S is determined (operations 641 and 642). Control device/controlled device 610 and a security manager 620 randomly select a session ID. According to other exemplary embodiments, IDs of the control device/con-

trolled device 610 and an ID of the security manager 620 may be used as the session ID. The control device/controlled device 610 transmit the session ID, ciphers, and an arbitrary Nonce R1 to the security manager 620 (operation 643). The ciphers include an identifier indicating that Pre-shared TLS implemented by a Session Resumption Protocol (SRP) is used. If required, the session ID may include the identifier.

[0059] The security manager 620 recognizes the use of a Pre-shared TLS protocol implemented by the SRP via the ciphers, and transmits a session ID, a cipher, an arbitrary Nonce R2, and hash value generated from a Pre-master secret S, control device/controlled device IDs, an arbitrary Nonce R1, a security manager ID, and an arbitrary Nonce R2 to the control device/controlled device 610 (operation 644).

[0060] According to the hash values transmitted from the security manager 620, the control device/controlled device 610 confirms that the security manager 620 has the Pre-master secret S. When the confirmation is successfully finished, the control device/controlled device 610 calculates hash value by inputs of a Pre-master secret S, an arbitrary Nonce R1, and an arbitrary Nonce R2, and transmits the calculated hash value to the security manager 620 (operation 645). The security manager 620 transmits a finish message to the control device/controlled device 610, wherein the finish message indicates that the Pre-shared TLS protocol has been successfully completed (operation 646).

[0061] According to the current exemplary embodiment, in order to provide a secure communication between each of devices in a home network, a separate apparatus such as a security console based on an UPnP security architecture and a separate protocol such as a WPS protocol are not required, and also an additional out-of-band protocol is not required to be implemented, except for the TLS. That is, it is possible to easily implement communication security by slightly changing the existing TLS that is widely used. Also, the TLS is implemented by using a pre-shared symmetric key instead of using a public key certificate, thus, a complicated calculation necessary for an authentication process using a public key may be avoided.

[0062] FIG. 7 is a diagram illustrating a method of synchronizing authentication information between a security manager 710 and a sub-security manager 730 according to an exemplary embodiment of the present invention.

[0063] In a home network, a plurality of security managers may hierarchically exist, and each of the security managers manages authentication information about control devices and controlled devices managed by each of the security managers. When user authentication information is updated in a security manager existing in an upper layer, it is necessary to inform this update to a security manager existing in a lower layer of the upper layer so as to synchronize authentication information between the security managers.

[0064] A control device 720 discovers the security

manager 710 and the sub-security manager 730 (operation 741). In the case where a certificate, an SSK, or user authentication information is newly added, changed or deleted, the security manager 710 transmits a UserListUpdateNotify() message to the control device 720 via broadcast or multicast transmission (operation 742). The control device 720 receives this message, and then transmits a RequestUpdateUserList() message to the sub-security manager 730 or a device which needs an update (operation 743). If a plurality of control devices receive this message, the control device 720 transmits the RequestUpdateUserList() message after a predetermined lapse of time. If another control device transmits the RequestUpdateUserList() message first, the control device 720 cancels message transmission.

[0065] One of the sub-security manager 730 or the control device 720, which needs the update, sets a TLS connection based on a certificate with a corresponding security manager (operation 744), and starts the update by using an UpdateUserList() (operation 745). In order to verify validity of the certificate, a validity period of the certificate may be checked, whether the certificate is registered in a CRL may be checked, or the validity of the certificate may be provided from an OCSP service of a security manager.

[0066] FIG. 8 is a block diagram of a structure of a security manager apparatus 800, according to an exemplary embodiment of the present invention.

[0067] A user interface unit 810 externally receives PIN information of a device (e.g., from a user) so as to establish an SAC (refer to operation 122 of FIG. 1 and operation 232 of FIG. 2). In the case where a previously generated certificate is revoked, an identifier of the certificate to be revoked is externally input, or in the case where previously received user authentication information is changed or deleted, the user authentication information to be changed or deleted is externally input.

[0068] A control device interface unit 820 receives a control command from a control device 825. To be more specific, the control device interface unit 820 receives a control command allowing a certificate and an SSK, which are generated with respect to the control device 825 or a controlled device, to be transmitted to the control device 825 or the controlled device (refer to operation 125 of FIG. 1 and operation 235 of FIG. 2). Also, the control device interface unit 820 receives a control command allowing user authentication information to be transmitted to the controlled device (refer to operation 546 of FIG. 5), and receives user authentication information from the control device 825 via an SAC (refer to operation 435 of FIG. 4).

[0069] As illustrated in FIG. 6, a security channel establishing unit 830 sets an SAC by implementing TLS-PSK by using a pre-shared PIN (refer to operation 123 of FIG. 1, operation 233 of FIG. 2, operation 433 of FIG. 4, operation 547 of FIG. 5, and operation 699 of FIG. 6).

[0070] An authentication information transmitting unit 831 transmits authentication information to the control

device 825 or the controlled device via the SAC (refer to operation 126 of FIG. 1, and operation 236 of FIG. 2). Also, by way of a request from the control device 825, the authentication information transmitting unit 831 transmits stored user authentication information to the controlled device via the SAC (refer to operation 547 of FIG. 5).

[0071] A distribution unit 840 generates a MAC value by using the SSK, and then transmits the MAC value along with a message via broadcast/multicast transmission, thereby ensuring integrity of the message.

[0072] A CRL updating unit 841 externally receives an identifier, or adds a certificate to a CRL, wherein the certificate is about a device which has not been discovered during a predetermined period of time. An updated CRL is distributed to registered devices via the distribution unit 840.

[0073] A user authentication information updating unit 842 changes or deletes user authentication information externally received. Updated user authentication information is distributed to the registered devices via the distribution unit 840.

[0074] The invention can also be embodied as computer readable codes on a computer readable recording medium. The computer readable recording medium is any data storage device that can store data, which can be thereafter read by a computer system. Examples of the computer readable recording medium (including all devices having information process functions) include read-only memory (ROM), random-access memory (RAM), CD-ROMs, magnetic tapes, floppy disks, and optical data storage devices.

[0075] While this invention has been particularly shown and described with reference to exemplary embodiments thereof, it will be understood by those of ordinary skill in the art that various changes in form and details may be made therein without departing from the scope of the invention as defined by the appended claims. The exemplary embodiments should be considered in a descriptive sense only and not for purposes of limitation. Therefore, the scope of the invention is defined not by the detailed description of embodiments of the invention but by the appended claims, and all differences falling within the scope of the claims will be construed as being included within the scope of the present invention.

Claims

1. A method for managing authentication information in a home network comprising a control device (100, 200) and a controlled device (210), the method comprising the steps of:

receiving (122, 232), by a Security Manager (110, 220), Product Identification Number, PIN, information that is externally input and is an identifier allocated to the control device (100, 200)

- or the controlled device (210) at a time of manufacture; and transmitting (126, 236) authentication information from the Security Manager (110, 220) to the control device (100, 200) or the controlled device (210) via a Secure Authenticated Channel, SAC, generated (123, 233) by using a Transport Layer Security Pre-Shared Key ciphersuites, TLS-PSK, protocol implemented by using the PIN information, wherein the authentication information is necessary for a user to control the controlled device (210) via the control device (100, 200).
2. The method of claim 1, further comprising establishing (123, 233) the SAC by using a TLS-PSK protocol implemented by using a Transport Layer Security, TLS, session resumption protocol which uses a randomly generated value as a session identification, ID.
 3. The method of claim 2, wherein the establishing (123, 233) the SAC comprises:
 - calculating a hash value by using a pre-master secret generated from the PIN information; and transmitting the hash value to the control device (100, 200) or the controlled device (210), whereby the control device (100, 200) or the controlled device (210) authenticates the Security Manager (110, 220).
 4. The method of claim 1, wherein the authentication information comprises a certificate about the control device (100, 200) or the controlled device (210), a security key shared in the home network, and user authentication information about a user.
 5. The method of claim 4, further comprising:
 - generating (124, 234) the certificate about the control device (100, 200) or the controlled device (210); and receiving the user authentication information from the control device (100, 200) via the SAC.
 6. The method of claim 4, further comprising:
 - adding the certificate to a Certificate Revocation List, CRL, wherein the certificate is about a device corresponding to an identifier that is externally input or a device that is not discovered during a predetermined period of time; and distributing the CRL to a plurality of registered control devices and controlled devices.
 7. The method of claim 4, further comprising:
 - changing or deleting user authentication information that is externally input; and distributing the changed or deleted user authentication information to the plurality of registered control devices and controlled devices.
 8. The method of claim 6, wherein the distributing the CRL comprises:
 - generating a Message Authentication Code, MAC, value by using the security key shared in the home network; and transmitting the MAC value along with a message via broadcast or multicast transmission.
 9. The method of claim 7, wherein the distributing the changed or deleted user authentication information comprises:
 - generating a Message Authentication Code, MAC, value by using the security key shared in the home network; and transmitting the MAC value along with a message via broadcast or multicast transmission.
 10. The method of claim 1, wherein the method is performed by the Security Manager (110, 220), and the Security Manager (110, 220) is selected from among a plurality of security managers according to a predetermined priority order.
 11. The method of claim 1, further comprising:
 - requesting update of information to a sub-security manager, which manages authentication information in a lower layer of management, via the control device (100, 200) if authentication information is newly added, changed or deleted; establishing the SAC with the sub-security manager; and transmitting the newly added, changed or deleted authentication information to the sub-security manager.
 12. The method according to any one of claims 1 to 11, wherein the externally input PIN information is input by a user.
 13. An apparatus (800) adapted for managing authentication information in a home network comprising a control device (100, 200) and a controlled device (210), the apparatus comprising:
 - a user interface unit (810) adapted for receiving Product Identification Number, PIN, information that is externally input and is an identifier allocated to the control device (100, 200) or the controlled device (210) at a time of manufacture;

and

an authentication information transmitting unit (831) adapted for transmitting authentication information to the control device (100, 200) or the controlled device (210) via a Secure Authenticated Channel, SAC, generated by using a Transport Layer Security Pre-Shared Key ciphersuites, TLS-PSK, protocol implemented by using the PIN information, wherein the authentication information is necessary for a user to control the controlled device (210) via the control device (100, 200).

14. The apparatus of claim 12, further comprising a security channel establishing unit (830) adapted for establishing the SAC by using a TLS-PSK protocol implemented by using a Transport Layer Security, TLS, session resumption protocol which uses a randomly generated value as a session identification, ID.

15. The apparatus of claim 12, wherein the authentication information comprises a certificate about the control device (100, 200) or the controlled device (210), a security key shared in the home network, and user authentication information about a user.

16. The apparatus according to any one of claims 13 to 15, wherein the externally input PIN information is input by a user.

17. A recording medium having recorded thereon a computer program for executing a method for managing authentication information in a home network comprising a control device (100, 200) and a controlled device (210), the method comprising the steps of:

receiving (122, 232), by a Security Manager (110, 220), Product Identification Number, PIN, information that is externally input and is an identifier allocated to the control device (100, 200) or the controlled device (210) at a time of manufacture; and

transmitting (126, 236) authentication information from the Security Manager (110, 220) to the control device (100, 200) or the controlled device (210) via a Secure Authenticated Channel, SAC, generated (123, 233) by using a Transport Layer Security Pre-Shared Key ciphersuites, TLS-PSK, protocol implemented by using the PIN information, wherein the authentication information is necessary for a user to control the controlled device (210) via the control device (100, 200).

18. The recording medium according to claim 17, wherein the externally input PIN information is input by a user.

Patentansprüche

1. Verfahren zum Verwalten von Authentifizierungsinformationen in einem Heimnetzwerk, das eine Steuervorrichtung (100, 200) und eine gesteuerte Vorrichtung (210) umfasst, wobei das Verfahren folgende Schritte umfasst:

Empfangen (122, 232) durch einen Sicherheitsmanager (110, 220) von Informationen einer Produktidentifikationsnummer, PIN, die extern eingegeben wird und eine Kennung ist, die der Steuervorrichtung (100, 200) oder der gesteuerten Vorrichtung (210) zum Zeitpunkt der Herstellung zugeordnet wird; und

Übertragen (126, 236) der Authentifizierungsinformationen von dem Sicherheitsmanager (110, 220) zu der Steuervorrichtung (100, 200) oder der gesteuerten Vorrichtung (210) über einen sicheren authentifizierten Kanal (SAC - Secure Authenticated Channel), der mit Hilfe eines Ciphersuite-Protokolls mit zuvor vereinbartem gemeinsamem Schlüssel zur Übertragungsschichtsicherheit (TLS-PSK - Transport Layer Security Pre-Shared Key) erzeugt wird (123, 233), das mit Hilfe der PIN Informationen implementiert wird, wobei die Authentifizierungsinformationen notwendig sind, damit ein Benutzer die gesteuerte Vorrichtung (210) über die Steuervorrichtung (100, 200) steuern kann.

2. Verfahren nach Anspruch 1, das ferner das Einrichten (123, 233) des SAC unter Verwendung eines TLS-PSK-Protokolls umfasst, das mit Hilfe eines Sitzungswiederaufnahmeprotokolls einer Transport Layer Security, TLS, implementiert wird, das einen zufällig erzeugten Wert als Sitzungskennung, ID, verwendet.

3. Verfahren nach Anspruch 2, wobei das Einrichten (123, 233) des SAC Folgendes umfasst:

Berechnen eines Hash-Wertes unter Verwendung eines Pre-Master-Secret, das aus den PIN-Informationen erzeugt wird; und Senden des Hash-Wertes zur Steuervorrichtung (100, 200) oder zur gesteuerten Vorrichtung (210), wodurch die Steuervorrichtung (100, 200) oder die gesteuerte Vorrichtung (210) den Sicherheitsmanager (110, 220) authentifiziert.

4. Verfahren nach Anspruch 1, wobei die Authentifizierungsinformationen Folgendes umfassen: ein Zertifikat über die Steuervorrichtung (100, 200) oder die gesteuerte Vorrichtung (210), einen Sicherheitsschlüssel, der in dem Heimnetzwerk gemeinsam genutzt wird, und die Benutzerauthentifizierungsinformationen über einen Benutzer.

5. Verfahren nach Anspruch 4, das ferner Folgendes umfasst:

Erzeugen (124, 234) des Zertifikats der Steuervorrichtung (100, 200) oder der gesteuerten Vorrichtung (210); und
Empfang der Benutzerauthentifizierungsinformationen von der Steuervorrichtung (100, 200) über den SAC.

6. Verfahren nach Anspruch 4, das ferner Folgendes umfasst:

Hinzufügen des Zertifikats zu einer Zertifikatswiderrufliste (Certificate Revocation List - CRL), wobei das Zertifikat Folgendes betrifft: eine Vorrichtung, die einer extern eingegebenen Kennung entspricht, oder eine Vorrichtung, die während einer vorbestimmten Zeit nicht entdeckt wird; und
Verteilen der CRL an eine Vielzahl von registrierten Steuervorrichtungen und gesteuerten Vorrichtungen.

7. Verfahren nach Anspruch 4, das ferner Folgendes umfasst:

Ändern oder Löschen von Benutzerauthentifizierungsinformationen, die extern eingegeben werden; und
Verteilen der geänderten oder gelöschten Benutzerauthentifizierungsinformationen an die Vielzahl der registrierten Steuervorrichtungen und gesteuerten Vorrichtungen.

8. Verfahren nach Anspruch 6, wobei das Verteilen der CRL Folgendes umfasst:

Erzeugen eines Wertes eines Nachrichten-Authentifizierungscodes (Message Authentication Code - MAC) mit Hilfe des Sicherheitsschlüssels, der in dem Heimnetzwerk gemeinsam genutzt wird; und
Übertragen des MAC-Wertes zusammen mit einer Nachricht über Rundfunk- oder Multicast-Übertragung.

9. Verfahren nach Anspruch 7, wobei die Verteilung der geänderten oder gelöschten Benutzerauthentifizierungsinformationen Folgendes umfasst:

Erzeugen eines Wertes eines Nachrichten-Authentifizierungscodes (Message Authentication Code - MAC) mit Hilfe des Sicherheitsschlüssels, der in dem Heimnetzwerk gemeinsam genutzt wird; und
Übertragen des MAC-Wertes zusammen mit einer Nachricht über Rundfunk- oder Multicast-

Übertragung.

10. Verfahren nach Anspruch 1, wobei das Verfahren durch den Sicherheitsmanager (110, 220) ausgeführt wird und der Sicherheitsmanager (110, 220) aus einer Vielzahl von Sicherheitsmanagern gemäß einer vorbestimmten Prioritätenfolge ausgewählt wird.

11. Verfahren nach Anspruch 1, das ferner Folgendes umfasst:

Anfordern einer Aktualisierung von Informationen eines Untersicherheitsmanagers, der Authentifizierungsinformationen in einer unteren Verwaltungsschicht über die Steuervorrichtung (100, 200) verwaltet, wenn Authentifizierungsinformationen neu hinzugefügt, geändert oder gelöscht werden;
Einrichten des SAC mit dem Untersicherheitsmanager; und
Senden der neu hinzugefügten, geänderten oder gelöschten Authentifizierungsinformationen zu dem Untersicherheitsmanager.

12. Verfahren nach einem der Ansprüche 1 bis 11, wobei die extern eingegebenen PIN-Informationen von einem Benutzer eingegeben werden.

13. Vorrichtung (800) zum Verwalten von Authentifizierungsinformationen in einem Heimnetzwerk, das eine Steuervorrichtung (100, 200) und eine gesteuerte Vorrichtung (210) umfasst, wobei die Vorrichtung Folgendes umfasst:

eine Benutzerschnittstelleneinheit (810), die dafür ausgelegt ist, Informationen einer Produktidentifikationsnummer, PIN, zu empfangen, die extern eingegeben wird und eine Kennung ist, die der Steuervorrichtung (100, 200) oder der gesteuerten Vorrichtung (210) zum Zeitpunkt der Herstellung zugeordnet wird; und
eine Übertragungseinheit (831) für Authentifizierungsinformationen, die dafür ausgelegt ist, Authentifizierungsinformationen zur der Steuervorrichtung (100, 200) oder der gesteuerten Vorrichtung (210) über einen sicheren authentifizierten Kanal (SAC - Secure Authenticated Channel) zu senden, der mit Hilfe eines Ciphersuite-Protokolls mit zuvor vereinbartem gemeinsamem Schlüssel zur Übertragungsschichtsicherheit (TLS-PSK - Transport Layer Security Pre-Shared Key) erzeugt wird, das mit Hilfe der PIN Informationen implementiert wird, wobei die Authentifizierungsinformationen notwendig sind, damit ein Benutzer die gesteuerte Vorrichtung (210) über die Steuervorrichtung (100, 200) steuern kann.

14. Vorrichtung nach Anspruch 12, die ferner eine Einrichtungseinheit (830) für einen Sicherheitskanal umfasst, die dafür ausgelegt ist, den SAC unter Verwendung eines TLS-PSK-Protokolls einzurichten, das mit Hilfe eines Sitzungswiederaufnahmeprotokolls einer Transport Layer Security, TLS, implementiert wird, das einen zufällig erzeugten Wert als Sitzungskennung, ID, verwendet. 5
15. Vorrichtung nach Anspruch 12, wobei die Authentifizierungsinformationen Folgendes umfassen: ein Zertifikat über die Steuervorrichtung (100, 200) oder die gesteuerte Vorrichtung (210), einen Sicherheits- 10 schlüssel, der in dem Heimnetzwerk gemeinsam genutzt wird, und die Benutzerauthentifizierungsinformationen über einen Benutzer. 15
16. Vorrichtung nach einem der Ansprüche 13 bis 15, wobei die extern eingegebenen PIN-Informationen von einem Benutzer eingegeben werden. 20
17. Aufzeichnungsmedium, auf dem ein Computerprogramm zum Ausführen eines Verfahrens zum Ver- 25 halten von Authentifizierungsinformationen in einem Heimnetzwerk aufgezeichnet ist, das eine Steuervorrichtung (100, 200) und eine gesteuerte Vorrichtung (210) umfasst, wobei das Verfahren folgende Schritte umfasst:
- Empfangen (122, 232) durch einen Sicherheits- 30 manager (110, 220) von Informationen einer Produktidentifikationsnummer, PIN, die extern eingegeben wird und eine Kennung ist, die der Steuervorrichtung (100, 200) oder der gesteuerten Vorrichtung (210) zum Zeitpunkt der Herstellung zugeordnet wird; und Übertragen (126, 35 236) der Authentifizierungsinformationen von dem Sicherheitsmanager (110, 220) zu der Steuervorrichtung (100, 200) oder der gesteuerten Vorrichtung (210) über einen sicheren authentifizierten Kanal (SAC - Secure Authentica- 40 ticated Channel), der mit Hilfe eines Ciphersuite-Protokolls mit zuvor vereinbartem gemeinsamem Schlüssel zur Übertragungsschichtssicherheit (TLS-PSK - Transport Layer Security Pre-Shared Key) erzeugt wird (123, 233), das mit Hilfe der PIN Informationen implementiert wird, wobei die Authentifizierungsinformationen not- 45 wendig sind, damit ein Benutzer die gesteuerte Vorrichtung (210) über die Steuervorrichtung (100, 200) steuern kann. 50
18. Aufzeichnungsmedium nach Anspruch 17, wobei die extern eingegebenen PIN-Informationen von einem Benutzer eingegeben werden. 55

Revendications

1. Un procédé de gestion d'informations d'authentification dans un réseau domestique comprenant un dispositif de commande (100, 200) et un dispositif commandé (210), le procédé comprenant the les opérations suivantes :

la réception (122, 232), par un gestionnaire de sécurité (110, 220), d'informations de numéro d'identification de produit, PIN, qui sont saisies de manière externe et sont un identifiant attribué au dispositif de commande (100, 200) ou au dispositif commandé (210) au moment de la fabrication, et
la transmission (126, 236) d'informations d'authentification du gestionnaire de sécurité (110, 220) au dispositif de commande (100, 200) ou au dispositif commandé (210) par l'intermédiaire d'un canal authentifié sécurisé, SAC, générées (123, 233) au moyen d'un protocole TLS-PSK, suites de chiffres de clé pré-partagée - sécurité de couche de transport, mis en oeuvre au moyen des informations PIN, où les informations d'authentification sont nécessaires à un utilisateur pour la commande du dispositif commandé (210) par l'intermédiaire du dispositif de commande (100, 200).
2. Le procédé selon la Revendication 1, comprenant en outre l'établissement (123, 233) du SAC au moyen d'un protocole TLS-PSK mis en oeuvre au moyen d'un protocole de reprise de session de sécurité de couche de transport, TLS, qui utilise une valeur générée de manière aléatoire en tant qu'identifiant de session, ID.
3. Le procédé selon la Revendication 2, où l'établissement (123, 233) du SAC comprend :

le calcul d'une valeur de hachage au moyen d'un secret pré-maître généré à partir des informations PIN, et
la transmission de la valeur de hachage au dispositif de commande (100, 200) ou au dispositif commandé (210), grâce à quoi le dispositif de commande (100, 200) ou le dispositif commandé (210) authentifie le gestionnaire de sécurité (110, 220).
4. Le procédé selon la Revendication 1, où les informations d'authentification comprennent un certificat relatif au dispositif de commande (100, 200) ou au dispositif commandé (210), une clé de sécurité partagée dans le réseau domestique et des informations d'authentification d'utilisateur relatives à un utilisateur.

5. Le procédé selon la Revendication 4, comprenant en outre :
- la génération (124, 234) du certificat relatif au dispositif de commande (100, 200) ou au dispositif commandé (210), et
la réception des informations d'authentification d'utilisateur à partir du dispositif de commande (100, 200) par l'intermédiaire du SAC.
6. Le procédé selon la Revendication 4, comprenant en outre :
- l'ajout du certificat à une liste de révocation de certificats, CRL, où le certificat porte sur un dispositif correspondant à un identifiant qui est saisi de manière externe ou un dispositif qui n'est pas découvert au cours d'une période de temps prédéterminée, et
la distribution de la CRL à une pluralité de dispositifs de commande et de dispositifs commandés enregistrés.
7. Le procédé selon la Revendication 4, comprenant en outre :
- la modification ou la suppression d'informations d'authentification d'utilisateur qui sont saisies de manière externe, et
la distribution des informations d'authentification d'utilisateur modifiées ou supprimées à la pluralité de dispositifs de commande et de dispositifs commandés enregistrés.
8. Le procédé selon la Revendication 6, où la distribution de la CRL comprend :
- la génération d'une valeur de code d'authentification de message, MAC, au moyen de la clé de sécurité partagée dans le réseau domestique, et
la transmission de la valeur MAC conjointement avec un message par l'intermédiaire d'une transmission de radiodiffusion ou de multidiffusion.
9. Le procédé selon la Revendication 7, où la distribution des informations d'authentification d'utilisateur modifiées ou supprimées comprend :
- la génération d'une valeur de code d'authentification de message, MAC, au moyen de la clé de sécurité partagée dans le réseau domestique, et
la transmission de la valeur MAC conjointement avec un message par l'intermédiaire d'une transmission de radiodiffusion ou de multidiffusion.
10. Le procédé selon la Revendication 1, où le procédé est exécuté par le gestionnaire de sécurité (110, 220), et le gestionnaire de sécurité (110, 220) est sélectionné parmi une pluralité de gestionnaires de sécurité selon un ordre de priorité prédéterminé.
11. Le procédé selon la Revendication 1, comprenant en outre :
- la demande d'une mise à jour d'informations à un sous-gestionnaire de sécurité qui gère des informations d'authentification dans une couche de gestion inférieure par l'intermédiaire du dispositif de commande (100, 200) si des informations d'authentification sont nouvellement ajoutées, modifiées ou supprimées, l'établissement du SAC avec le sous-gestionnaire de sécurité, et
la transmission des informations d'authentification nouvellement ajoutées, modifiées ou supprimées au sous-gestionnaire de sécurité.
12. Le procédé selon l'une quelconque des Revendications 1 à 11, où les informations PIN saisies de manière externe sont saisies par un utilisateur.
13. Un appareil (800) adapté à la gestion d'informations d'authentification dans un réseau domestique comprenant un dispositif de commande (100, 200) et un dispositif commandé (210), l'appareil comprenant :
- une unité d'interface utilisateur (810) adaptée à la réception d'informations de numéro d'identification de produit, PIN, qui sont saisies de manière externe et qui sont un identifiant attribué au dispositif de commande (100, 200) ou au dispositif commandé (210) au moment de la fabrication, et
une unité de transmission d'informations d'authentification (831) adaptée à la transmission d'informations d'authentification au dispositif de commande (100, 200) ou au dispositif commandé (210) par l'intermédiaire d'un canal authentifié sécurisé, SAC, générées au moyen d'un protocole de suites de chiffres de clé pré-partagée - sécurité de couche de transport, TLS-PSK, mis en oeuvre au moyen des informations PIN, où les informations d'authentification sont nécessaires à un utilisateur pour la commande du dispositif commandé (210) par l'intermédiaire du dispositif de commande (100, 200).
14. L'appareil selon la Revendication 12, comprenant en outre une unité d'établissement de canal de sécurité (830) adaptée à l'établissement du SAC au moyen d'un protocole TLS-PSK mis en oeuvre au moyen d'un protocole de reprise de session de sécurité de couche de transport, TLS, qui utilise une

valeur générée de manière aléatoire en tant qu'identifiant de session, ID.

15. L'appareil selon la Revendication 12, où les informations d'authentification comprennent un certificat relatif au dispositif de commande (100, 200) ou au dispositif commandé (210), une clé de sécurité partagée dans le réseau domestique et des informations d'authentification d'utilisateur relatives à un utilisateur. 5
10
16. L'appareil selon l'une quelconque des Revendications 13 à 15, où les informations PIN saisies de manière externe sont saisies par un utilisateur. 15
17. Un support d'enregistrement possédant enregistré sur celui-ci un programme informatique destiné à l'exécution d'un procédé de gestion d'informations d'authentification dans un réseau domestique comprenant un dispositif de commande (100, 200) et un dispositif commandé (210), le procédé comprenant les opérations suivantes : 20
 - la réception (122, 232), par un gestionnaire de sécurité (110, 220), d'informations de numéro d'identification de produit, PIN, qui sont saisies de manière externe et sont un identifiant attribué au dispositif de commande (100, 200) ou au dispositif commandé (210) au moment de la fabrication, et 25
30
 - la transmission (126, 236) d'informations d'authentification du gestionnaire de sécurité (110, 220) au dispositif de commande (100, 200) ou au dispositif commandé (210) par l'intermédiaire d'un canal authentifié sécurisé, SAC, générées (123, 233) au moyen d'un protocole de suites de chiffres de clé pré-partagée - sécurité de couche de transport, TLS-PSK, mis en oeuvre au moyen des informations PIN, où les informations d'authentification sont nécessaires à un utilisateur pour la commande du dispositif commandé (210) par l'intermédiaire du dispositif de commande (100, 200). 35
40
18. Le support d'enregistrement selon la Revendication 17, où les informations PIN saisies de manière externe sont saisies par un utilisateur. 45

50

55

FIG. 1

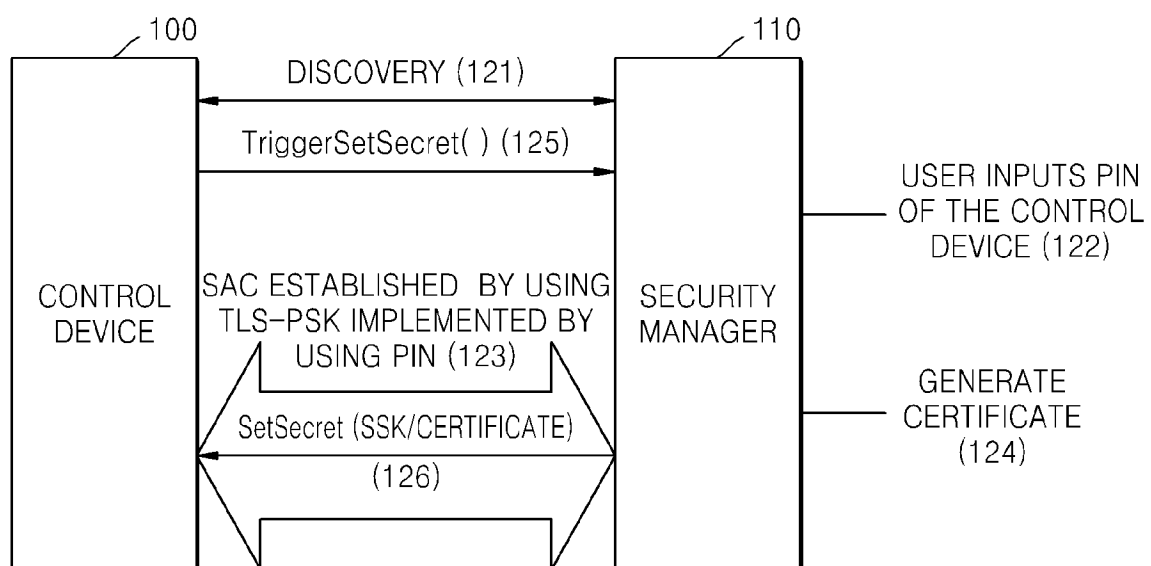


FIG. 2

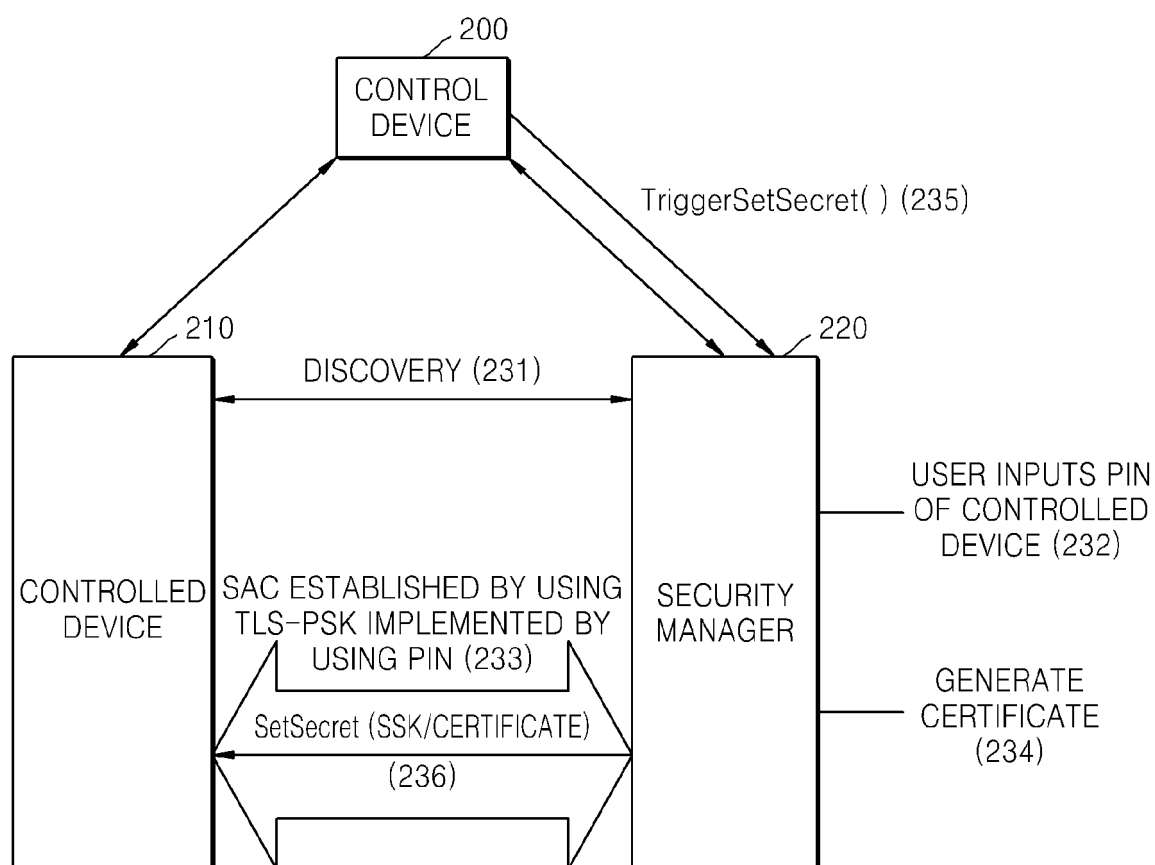


FIG. 3

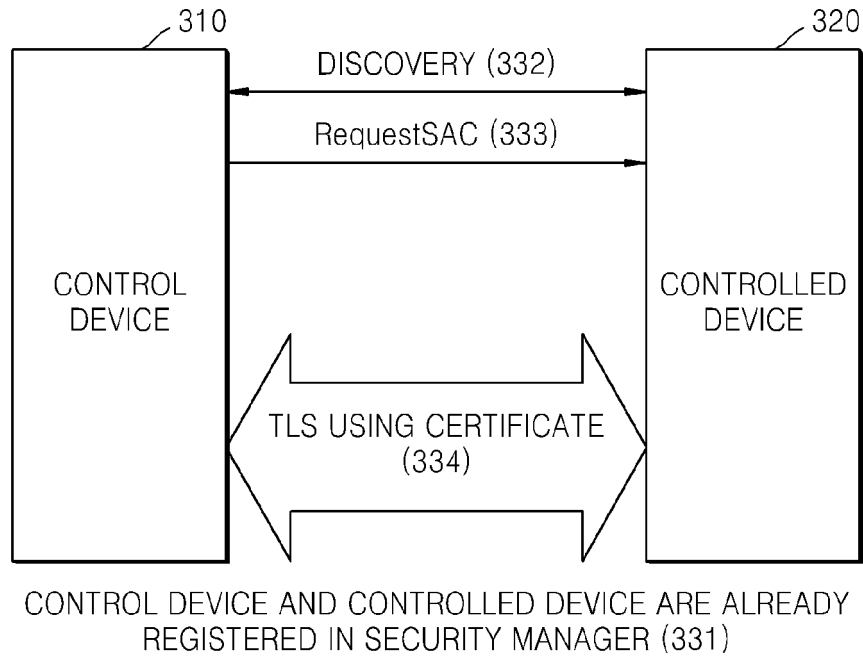


FIG. 4

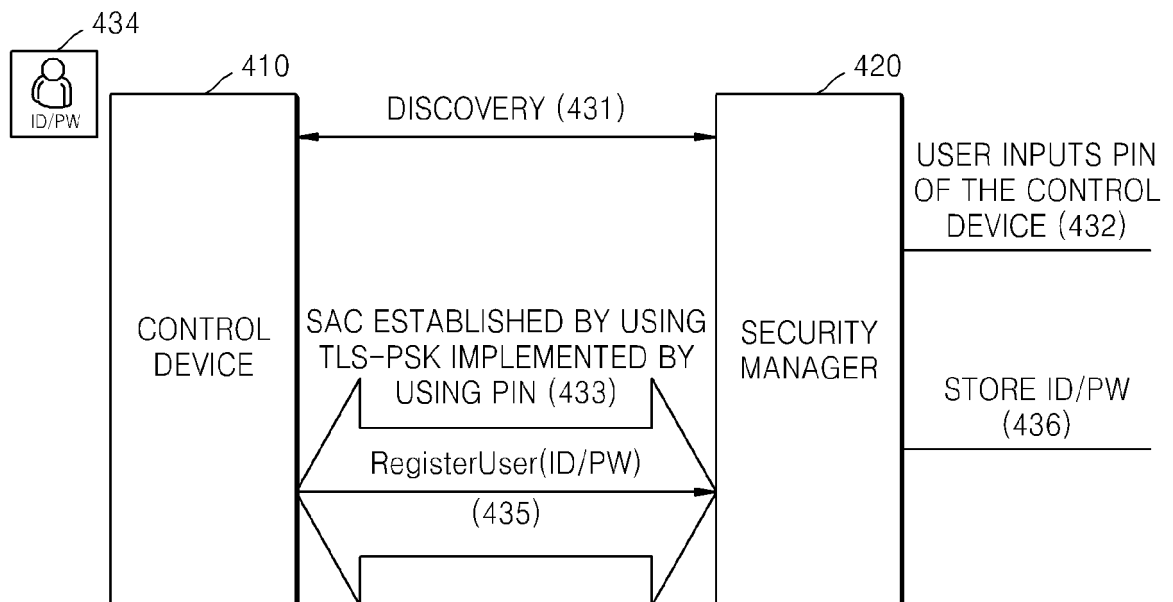


FIG. 5

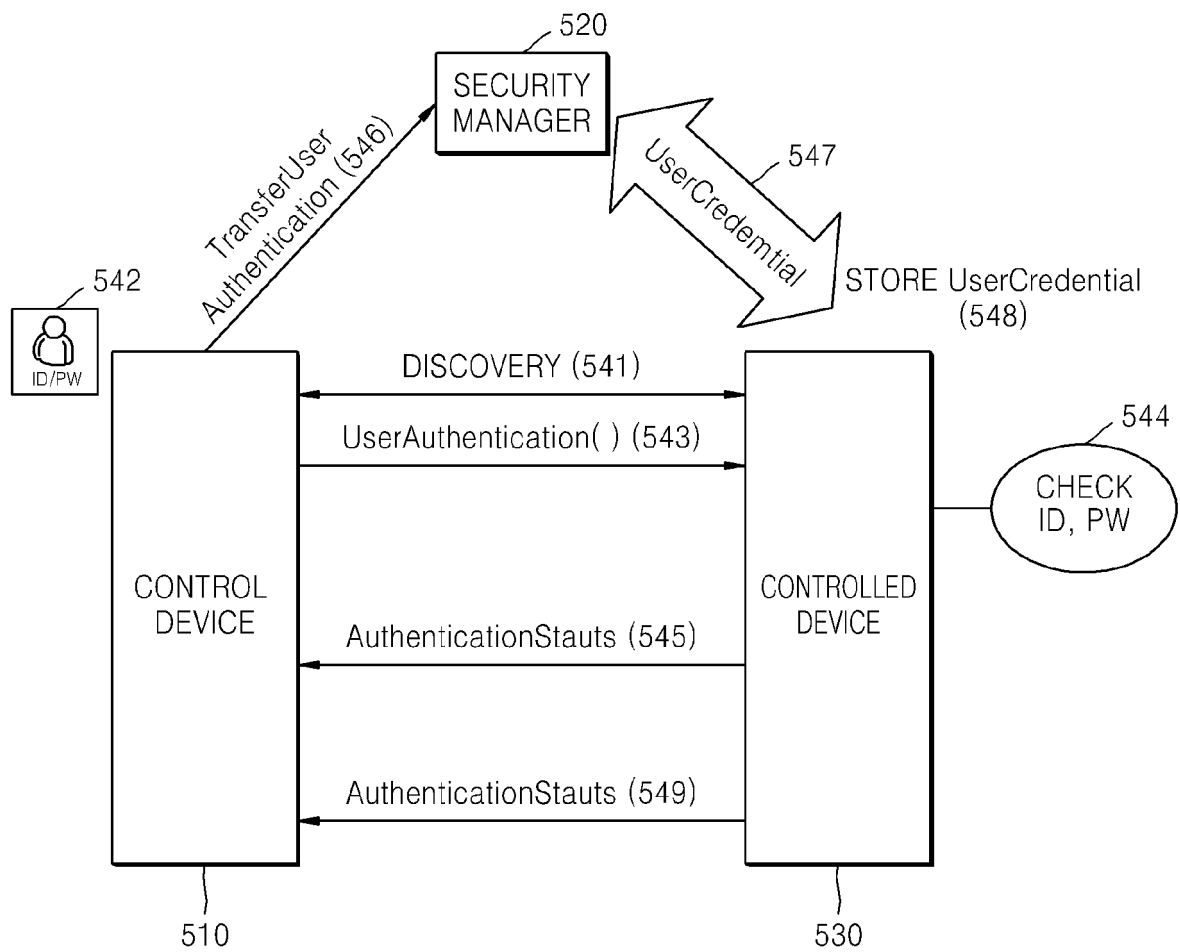
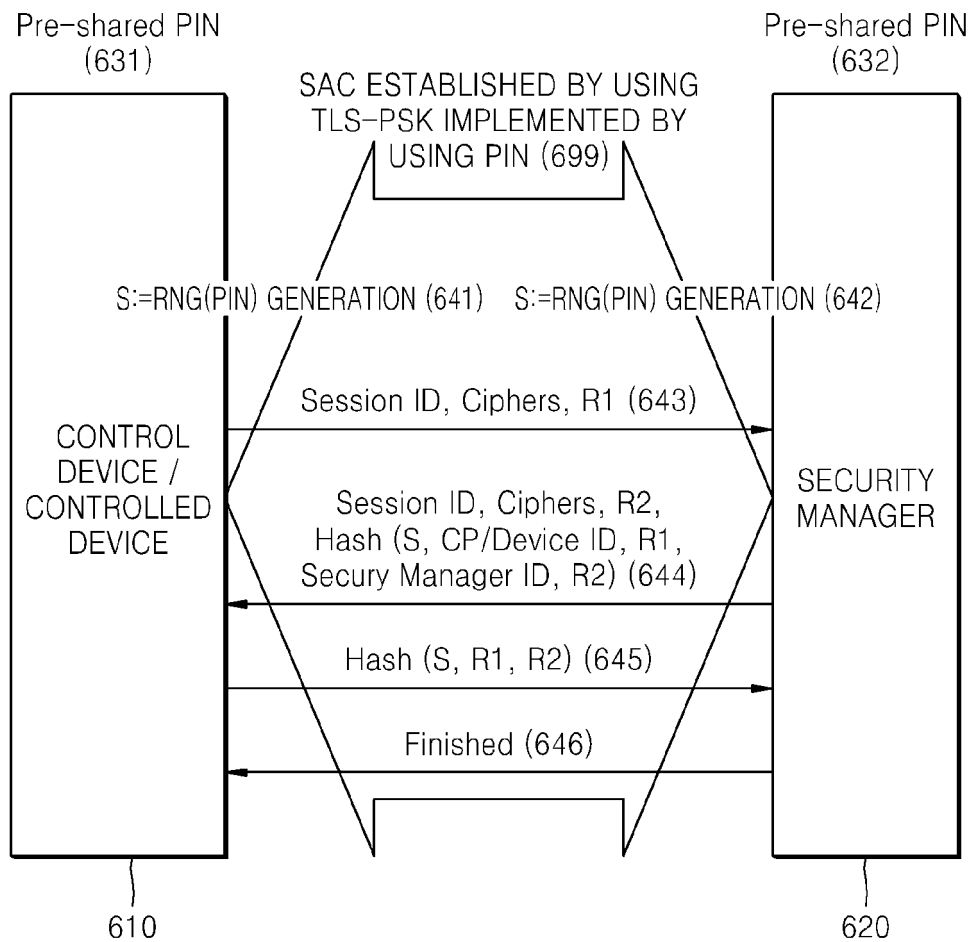


FIG. 6



Session ID: RANDOMLY SELECTED 32 BYTES
 Nonce R1/R2: 32 BYTES

FIG. 7

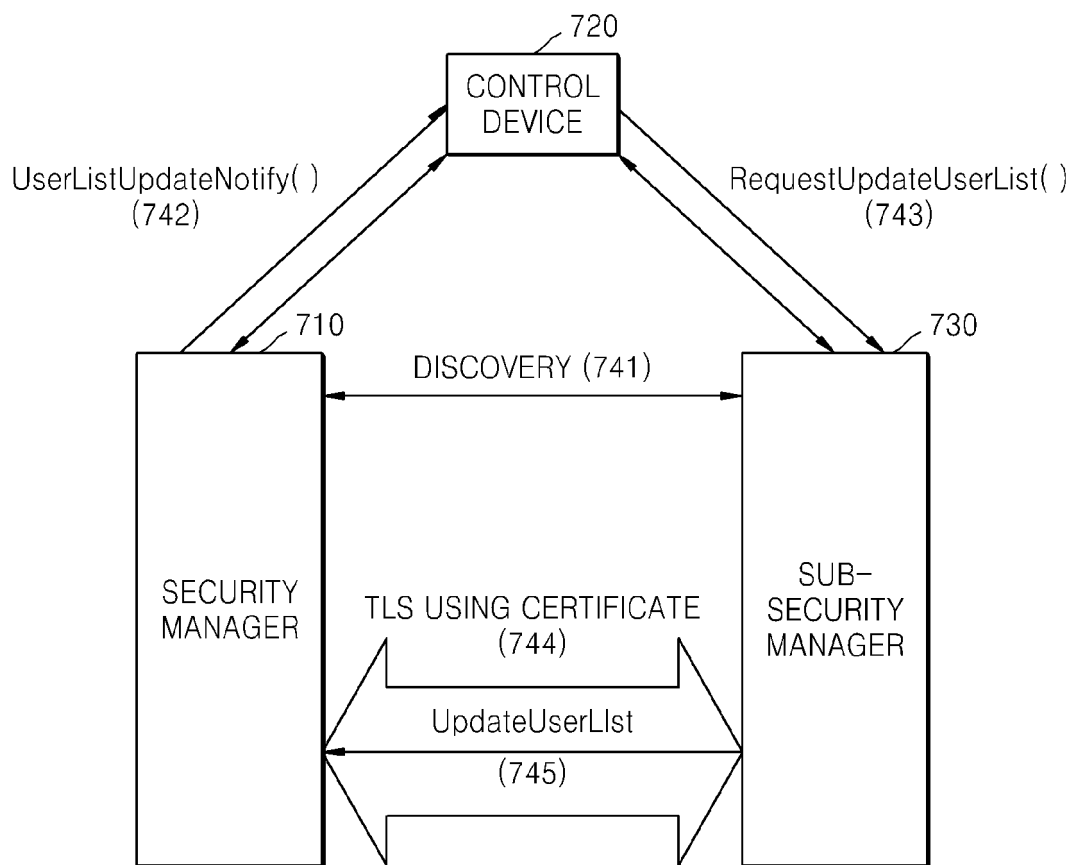
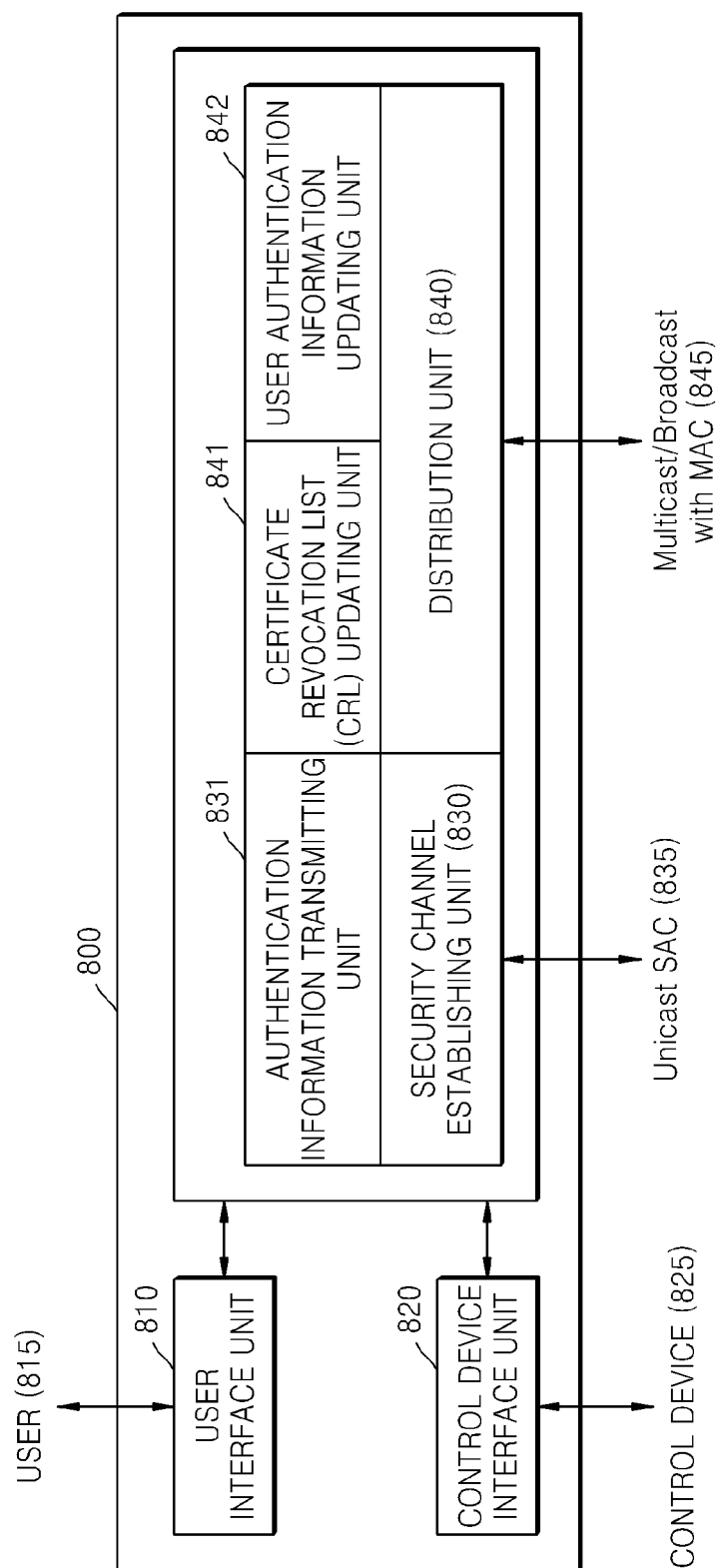


FIG. 8



REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Non-patent literature cited in the description

- Home Network Device Authentication: Device Authentication Framework and Device Certificate Profile. **YUN-KYUNG LEE et al.** Advances in Web and Network Technologies, and Information Management, Lecture Notes in Computer Science. Springer, 573-582 [0008]
- Use Cases of Implicit Authentication and Key Establishment with Sender and Receiver ID Binding. **DAN FORSBERG.** World of Wireless, Mobile and Multimedia Networks. IEEE International Symposium, 01 June 2007, 1-8 [0009]